I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted today via the Office electronic filing system in accordance with 37 CFR §1.6 (a)(4).

Date: June 9/2010 Signature:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/702,540 Confirmation No. 8250
Applicant : Vincent So
Filed : November 7, 2003
TC/A.U. : 3621
Examiner : Charles C. Agwumezie

Docket No. : 79865-5
Customer No. : 07380

MAILSTOP AF
EXPEDITED HANDLING REQUESTED

Commissioner for Patents
Alexandria, VA 22313-1450
U.S.A.
Dear Sir:

APPELANT'S REQUEST FOR REINSTATEMENT OF APPEAL AND SUPPLEMENTAL BRIEF UNDER 37 C.F.R. 41.37

Applicant hereby requests reinstatement of the Appeal for which a Notice of Appeal was originally submitted on September 17, 2009. The following is the Appellant's Supplemental Brief, submitted under the provisions of 37 C.F.R. 41.37. Please be advised that an appeal fee in the amount of $250.00 for filing an Appeal Brief and an appeal fee in the amount of $250 for filing a Notice of Appeal have previously been paid on September 19, 2007 and July 27, 2007 respectively, and the $20 difference in each fee due to an increase in the appeal fees were paid pursuant to 37 C.F.R. 41.20 and 35 U.S.C. 134 on December 10, 2009 and September 17, 2009 respectively.

This Supplemental Brief includes everything from Applicant's Appeal Brief filed December 10, 2009, and includes content that addresses a further ground of rejection raised by the Examiner. The new ground is listed as item 1 under the "Grounds of Rejection to be Reviewed on Appeal" section, and is discussed under item 1 of the "Arguments" section.

Table of Contents

Real Party in Interest

The real party in interest is the applicant, i.e. Vincent So, current address710 Bowercrest Crescent, Gloucester, Ontario, Canada K1V 2M2.

Related Appeals and Interferences

There are no related appeals or interferences that will directly affect, be directly affected by, or have a bearing on the present appeal.

Status of the Claims

Claims 2, 3, 24-33 and 37 are cancelled.

Claims 1, 4-15, 35-36 and 38-53 are withdrawn.

Claims 16-23, 34 and 54-56 remain in the application. Claims 16-23, 34 and 54-56 stand rejected and the rejection is appealed.

An Appendix containing a copy of the appealed claims is attached hereto.

Status of Amendments

No amendments have been filed subsequent to the Final Action dated June 22, 2009. Accordingly, it is Applicant's understanding that the claims presently on file correspond to the listing of claims filed in the Office Action response dated February 19, 2009.

Summary of the Claimed Subject Matter

Claim 16 is and independent claim that relates to "[a] method of receiving and controlling playback of video data content at a customer processing platform". Figure 3 illustrates a flowchart of a method that includes receiving and controlling playback of video data content at a customer processing platform. Receiving encrypted video data content at a customer processing platform is also described with reference to Figure 1, beginning on page 11, line 23 and with reference to Figure 4, beginning on page 26, line 22. Controlling playback of data content at a customer processing platform is described beginning on page 21, line 23. As noted above with reference to Figure 1, a customer processing platform may, for example, be implemented as part of the computer system 78, 80 shown in Figure 4, or the computer system 14 shown in Figure 1.

Claim 16 recites that the method comprises: "receiving over a communications medium a plurality of encrypted sections of video data content, each of which has been encrypted using a respective encryption key".

With reference to, for example, page 31, lines 3-10 of the instant application, it is noted that encrypted video data content may be delivered by a wide variety of delivery mechanisms: broadcast communications, direct download, on CDs, DVDs, diskettes, memory cards, e-mail, peer-to-peer file sharing, etc. Accordingly, the communications medium may be any medium by which the encrypted video data content can be delivered/communicated to the customer processing platform. Encryption of sections of video data content using respective encryption keys is described, for example, with reference to step 27 of the flowchart of Figure 2 beginning on page 17, line 7, which states that "[a]t 27, encryption is applied to each of a plurality of sections of each video to be downloaded. For example, if a video is to be downloaded in four sections, then encryption is applied to each of the four sections in step 27".

In claim 16, the method is recited to also include:

"for each encrypted section:

receiving a respective decryption key in respect of the encrypted section before playback of a preceding encrypted section of the plurality of encrypted sections is complete;

decrypting and playing back the encrypted section using the respective decryption key; and

destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content".

Steps 37 to 44 of Figure 3 and the accompanying description on page 19, line 29 to page 20, line 7, relate to the delivery of a first decryption key for a first encrypted section, and the delivery of a second decryption key for a second encrypted section, once the first decryption key has been destroyed. Also as noted above, page 21, lines 3 to 22 clarify that, in some embodiments, the second decryption key may be delivered before the first key is destroyed, but that the first key is destroyed at least before all of the other decryption keys are obtained by the customer processing platform.

Claim 17 is dependent on claim 16. Claim 17 recites that the method of claim 16 further comprises "for each encrypted section: destroying decrypted video data content at the customer processing platform after completing playback of the encrypted section". Page 22, lines 7-12 state that in some embodiments, "a different key is transmitted to the customer at an appropriate time to enable the customer to use the next section of the data content, preferably without any interruption, and the first key and any related decrypted data content from the first section is destroyed at the customer's computer system" (emphasis added).

Claim 18 is dependent on claim 16. Claim 18 recites "wherein the communications medium is the public Internet". Delivery of encrypted data content via the

Internet is specifically discussed with reference to Figure 1 on page 8, lines 10-12 and with reference to Figure 4 on page 26, lines 1-4.

Claim 19 is dependent on claim 16. Claim 19 recites "wherein, for each encrypted section, the respective encryption key is the same as the respective decryption key". As noted above with reference to claim 9, symmetric encryption/decryption systems involve the use of the same key for encryption and decryption. On page 12, lines 5-6 it is stated that "[t]he secret decryption key is the same as the secret encryption key in symmetric encryption schemes". On page 14, lines 10-12, it is stated that "symmetric key cryptography involves the same keys for encryption and decryption operations".

Claim 20 is dependent on claim 16. Claim 20 recites "wherein receiving the plurality of encrypted sections of the video data content comprises receiving the plurality of encrypted sections of the video data content from another customer processing platform via a peer-to-peer network, and wherein, for each encrypted section, the decryption key is encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform". Peer to peer distribution of encrypted video data content, i.e. delivering encrypted video data content between customer processing platforms, is described with reference to the peer-to-peer network 86 shown in Figure 4, beginning on page 30, line 18, which states:

> "[i]n another operating mode, the download controllers 79 and 81 download encrypted data content from other sources than the service providers 66, 68, and 70, including other users.
>
> Peer-to-peer communication techniques, represented in FIG. 4 by the peer-to-peer network 86, are commonly used to share files between computer systems. Although data content is available through the service providers 66, 68, and 70, users are also encouraged to share encrypted data content with other users. For example, after encrypted data content is downloaded to the computer system 78 from the service provider 68, the computer system 78 effectively becomes another distribution point for the encrypted data content. Downloaded encrypted data

> content is then available to the computer system 80 and other computer systems through the peer-to-peer network 86. On-line file sharing services are among the most common means for sharing data between computer systems. However, it should be appreciated that downloaded encrypted data may be shared using other distribution channels, including but not limited to email and such portable storage media as CDs, DVDs, diskettes, and memory cards. Thus, the peer-to-peer network 86 is shown in FIG. 4 as one illustrative example of the many possible mechanisms for sharing encrypted data content between computer systems and users" (emphasis added).

The use of public/private cryptographic keys is discussed, for example, at page 12, lines 1-11 and at page 20, line 17 to page 21, line 2. For example, at page 20, lines 29-31 it is stated that "[i]n one embodiment, the key itself is encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer."

Claim 21 is dependent on claim 16. Claim 21 recites "[a] computer-readable medium storing instructions which, when executed by a customer processing platform, perform a method according to claim 16". On page 22, line 29 it is stated that in some embodiments, "[t]he foregoing systems and methods are implemented as a computer readable medium containing software code executable by a processing platform in an embodiment of the invention".

Claim 22 is dependent on claim 16. Claim 22 recites "wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform". Generating encryption keys using an identifier associated with the customer processing platform, such as an IP address, is described beginning on page 14, line 18, which states that "[s]everal options exist for determining customer processing platform-specific keys. Key determination based on unique customer processing platform identifiers is generally preferred so that each customer processing platform has a unique key or set of keys. A network address such as an IP address or hardware identifiers associated with a computer system upon which the customer processing platform is operating are two illustrative examples of possible unique identifiers" (emphasis added).

Claim 23 is dependent on claim 16. Claim 23 recites "wherein receiving each respective decryption key comprises receiving a transmission value that is determined based on the respective decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section: recovering the respective decryption key from the transmission value". A hardware identifier is one example of a unique identifier associated with a customer processing platform. Generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with a customer processing platform is discussed in detail beginning on page 15, line 3, which states that "[a]ccording to another embodiment, a decryption key is transformed at a data content provider using such a unique customer processing platform identifier. In a simple illustrative example of this embodiment, each decryption key A_n required to decrypt downloaded data content is transformed using a network address B associated with a user's computer system to generate a respective transmission value $C_n = A_n - B$." Reception of the transmission values at the customer processing platform is described beginning on page 15, line 10, which states that "[e]ach transmission value is then sent to the customer processing platform for decryption of encrypted blocks of the data content in the manner described herein. The customer processing platform then performs a reverse transformation on the transmission value to recover the decryption key, as $C_n + B = A_n$ in this example" (emphasis added).

Claim 34 is an independent claim that relates to "[a] method for controlling use of encrypted video data content downloaded to a customer data content processing device". Controlling use of encrypted data content is described beginning on page 19, line 29 with reference to the method steps 41-44 of Figure 3. Controlling use of encrypted data content may involve destruction of decryption keys and/or destruction of decrypted data content, as described, for example, on page 22, lines 7-12, which states that in some embodiments, "a different key is transmitted to the customer at an appropriate time to enable the customer to use the next section of the data content, preferably without any interruption, and the first key and any related decrypted data content from the first section is destroyed at the customer's computer system" (emphasis added).

A customer data content processing device may, for example, be implemented by the download controller 16 that is part of the computer system 14 shown in Figure 1, or as one of the download controllers 79, 81 that are part of the computer system 78, 80 shown in Figure 4.

In claim 34, it is recited that the method comprises: "receiving a request comprising customer verification information from a customer data content processing device". With reference to Figure 1, it is stated beginning on page 10, line 26 that

> "[a]ccording to one embodiment, the video download controller 16 includes a user or customer interface that facilitates the exchange of customer verification information and subsequent rental selection information between a customer, at the computer system 14, and the video server 10. Customer verification information includes such information as a network address of the computer system 14, a customer email address, or a customer or account identification number. Customer verification information is also stored at the video server 10 for all properly registered customers or subscribers. It should be appreciated that the customer verification information may include more than one type of customer-related information. For example, access to the video server 10 by any customer may be restricted to particular computers or locations where customer verification information includes both a customer ID and a network address. In this case, the video server 10 grants access to its data content only if a customer establishes a connection from a predetermined network address. However, more common password-based access control is also contemplated for the video server 10. In other embodiments, the network address of the computer system 14 is transferred to the video server 10 as a destination address for file downloading as described in further detail below, and access control is based on other customer verification information provided to the video server 10" (emphasis added).

In claim 34, it is also recited that the method includes "comparing the customer verification information with corresponding stored customer information; and where the customer verification information is consistent with the stored customer verification information:

billing a usage charge to an account of the customer; transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted video data content; and for each subsequent portion of the encrypted video data content: transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted video data content before playback of a preceding portion of the encrypted video data content is complete; and causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device only after at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device, such that contiguous playback of the portions of encrypted video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted video data content".

Comparing customer verification information with corresponding stored customer information is described beginning on page 18, line 15, which states that "[t]he data content provider server compares the customer verification information with locally stored corresponding customer verification information, and in the event that the locally stored and transmitted customer verification information match, the order information is processed. Ordered data content is encrypted with a set of digital keys such that different sections of the data content are encrypted with different keys. In a per-download billing model, a customer account is billed either at download time or upon confirmation that encrypted data content has been received".

Figure 3 illustrates a method of billing a user charge to a customer account (step 36) and transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted data content (step 37); and for each subsequent portion of the encrypted data: transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data (step 41); and causing a key for a preceding portion of the encrypted data to be destroyed (step 44). Delivery and destruction of decryption keys in a manner that facilitates contiguous playback of encrypted video data content is discussed, for example, at page 21, lines 3-22, which states:

> "Some time after the key is received, the customer starts to view the first section of the video. When, or preferably before, the video playback reaches a

> second section, the corresponding key for that section is transmitted to the customer and the key for the previous section is destroyed. Subsequent key transmission is in response to a timer at the video rental service provider's system or an automatic next key request generated at the customer's computer system when playback of a current section is completed or nearly completed. Timer-based automatic key requests are feasible, for example, where videos are segmented such that playback of each encrypted section takes a predetermined length of time. A key request timer is preferably adapted to stop if playback of a section is stopped, to prevent a premature key request before a subsequent section is ready for playback. In another embodiment, a key request is made when a predetermined control signal or data pattern, added to each section of the video by the video provider, is encountered during playback. The customer thus always has a key to unlock a current section, but should at no time possess the full set of keys" (emphasis added).

Claim 54 is dependent on claim 16. Claim 54 recites "wherein destroying the respective decryption key only after at least the respective decryption key in respect of the next encrypted section has been received comprises destroying the respective decryption key only after completing playback of the encrypted section and beginning contiguous playback of the next encrypted section." This claim covers embodiments in which the decryption key for a preceding encrypted section is destroyed only after decryption of a subsequent encrypted section has begun. This could potentially allow a user to review at least some portion of the previously decrypted video data content before playback of all of the encrypted data content is completed. However, the user would be prevented from reviewing all of the decrypted content, as the user's customer processing platform would at no time have simultaneous possession off all of the decryption keys. See page 21, lines 3-22 of the instant application quoted above.

Claim 55 is dependent on claim 16. Claim 55 recites that the method of claim 16 further comprises "for each encrypted section: requesting the respective decryption key in respect of a next encrypted section responsive to one of a control signal and a data pattern in the decrypted data content of an encrypted section that precedes the next encrypted section."

Similarly, claim 56 is dependent on claim 34. Claim 56 recites that the method of claim 34 further comprises "for each subsequent portion of the encrypted data: receiving a request from the customer data content processing device for the different key to decrypt the subsequent portion of the encrypted data, wherein the request was generated responsive to one of a control signal and a data pattern in the decrypted data content of a preceding portion of the encrypted data content during playback of the preceding portion of the encrypted data content." As noted above with reference to claim 34, on page 21, lines 17-20, it is stated that "[i]n another embodiment, a key request is made when a predetermined control signal or data pattern, added to each section of the video by the video provider, is encountered during playback".

Grounds of Rejection to be Reviewed on Appeal

The issues which are hereby presented for review are as follows:

1. whether claims 16-23, 34 and 54-56 are unpatentable under 35 U.S.C. 112, first paragraph.

2. whether claims 16-23, 34 and 54-56 are unpatentable under 35 U.S.C. 112, second paragraph.

3. whether claims 16-18, 21, 54 and 55 are unpatentable under 35 U.S.C. 103(a) over Feig et al. (U.S. Patent No. 7,251,833 B2) in view of Giroux et al. (U.S. Patent Application Publication No. 2002/0078361 A1);

4. whether claim 19 is unpatentable under 35 U.S.C. 103(a) over Feig et al. in view of Giroux et al. and further in view of Granger et al. (U.S. Patent No. 6,334,189 B1);

5. whether claims 22 and 23 are unpatentable under 35 U.S.C. 103(a) over Feig et al. in view of Giroux et al. and further in view of Watanabe et al. (U.S. Patent No. 7,114,073 B2);

6. whether claim 20 is unpatentable under 35 U.S.C. 103(a) over Feig et al. in view of Giroux et al. and further in view of Novak (U.S. Patent Application Publication No. 2003/0097655); and

7. whether claims 34 and 56 are unpatentable under 35 U.S.C. 103(a) over Peterka (U.S. Patent Application Publication No. 2002/0170053) in view of Feig et al. and further in view of Giroux et al.

Arguments

35 U.S.C. 112, First Paragraph

1. Whether claims 16-23, 34 and 54-56 are unpatentable under 35 U.S.C. 112, first paragraph.

On March 4, 2010, the Examiner contacted the Applicant's representative by telephone to discuss a new objection under 35 U.S.C. 112, first paragraph. More specifically, the Examiner indicated that he was prepared to allow the application, provided that Applicant's representative was able to identify some portion of the specification that provided support for the feature of independent claim 16 that reads "destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received", and corresponding features of independent claims 34 and 54. Applicant's representative requested time to review the application in order to provide a response to the Examiner's inquiry.

Applicant's representative reviewed the application and attempted to telephone the Examiner later in the day on March 4, 2010. However, the Examiner was unreachable by telephone, and therefore Applicant's representative left a voicemail for the Examiner, in which, as noted in paragraph 3 of the Final Action dated March 10, 2010, Applicant's representative advised the Examiner that Figure 3 of the instant application, and more particularly steps 37 to 44 of Figure 3, and the description of Figure 3 on pages 19 and 20 of the originally filed application are believed to provide clear support for the foregoing features of independent claims 16, 34 and 54. However, on March 10, 2010 the Examiner issued a Final Action that rejects claims 16-23, 34 and 54-56 under 35 U.S.C. 112, first paragraph, as the Examiner disagreed with the assertion that Figure 3 and its accompanying description at pages 19 to 20 clearly show that the decryption key for the current encrypted section is destroyed only after the decryption key for the next encrypted section has been received.

Applicant's representative was surprised by the conclusion reached by the Examiner and was able to reach the Examiner by telephone on June 4, 2010 in order to discuss the new rejection. During this conversation with the Examiner, the Examiner reiterated his position that Figure 3 of the instant application does not show a current key being destroyed only after the decryption key for the next encrypted section has been received. For justification of his conclusion, the Examiner stated that his interpretation of steps 41 and 44 of Figure 3 is such that the key for a current section is delivered in step 41, the current key is destroyed in step 44 and the algorithm loops back to step 39, and on to step 41 if there is a next encrypted section, such that the decryption key for the next encrypted section is delivered in step 41. Applicant advised the Examiner that this interpretation of Figure 3 completely ignores the fact that an initial decryption key, i.e. the respective decryption key for the "current" encrypted section, is delivered in step 37. The customer begins decrypting and watching the "current" encrypted section in step 38. A respective decryption key for the "next" encrypted section is then delivered to the customer processing platform (assuming that the "current" section is not the last section; see step 39) in step 41. At this point it should be readily apparent that the customer processing platform has received "a respective decryption key in respect of the next encrypted section". In steps 42 the process waits and checks that the "current" section has finished. At step 44, the "current" decryption key is destroyed and the algorithm returns to step 39 and the cycle repeats until the last section is detected at step 39 and the end is reached at step 40. Applicant submits that the order of steps 37, 41 and 44 clearly shows that the respective decryption key for the "current" encrypted section is destroyed in step 44 only after the respective decryption key for the "next" encrypted section has been received in step 41.

Applicant respectfully submits that the Examiner's assertions with regard to Figure 3 are completely contradicted by the actual Figure and its accompanying description. Some relevant portions of the description pertaining to Figure 3 are reproduced below to reinforce Applicant's assertions and to emphasize the completely erroneous nature of the Examiner's rejection under 35 U.S.C. 112, first paragraph.

The following are excerpts from the description of Figure 3 and similar embodiments on pages 19 to 21 of the instant application:

> At step 37, a first key which enables decryption or "unlocking" of a first section of the previously downloaded encrypted video content is sent to the customer. ... The first

section of the downloaded encrypted video is decrypted and displayed at step 38.

The next series of steps, 39 through 44, are repeated for each section of the video being viewed. In the event that the **current** section being viewed is the last section of the video, as determined at 39, the process ends at step 40. Otherwise, at step 41 the **next** key is sent to unlock the next section. Then a "holding pattern" is entered, as shown at 42 and 43, to await completion of playback of the **current** section. After the current section is finished, the **current** key is destroyed at step 44 and the **next** section is decrypted and viewed.

It should be appreciated that step 41 may instead be responsive to separate requests for keys for subsequent sections of a downloaded encrypted video, to enable a customer to stop a video playback and resume the playback operation at a later time. It is also contemplated that a playback operation need not necessarily start at a first section of a downloaded encrypted video. Incremental billing, including per-key billing for instance, may be preferred where such partial viewing is enabled.

In an example implementation of the above method, a customer establishes a connection with a video rental service provider's web site and makes a request to view a video. The customer is preferably required to enter certain information such as membership authorization, email address, network address, or credit card information in order to gain permission to view the video. After the customer information has been verified by the rental service provider, permission is granted and a charge is billed to the customer's account or credit card. A key for the first section is then transmitted to the user. In order to prevent use of the key by

> a party that intercepts the key transmission, a secure channel or transfer mechanism is preferred. In one embodiment, the key itself is encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer. Other secure transfer mechanisms will be apparent to those skilled in the art.
>
> Some time after the key is received, the customer starts to view the first section of the video. When, or preferably before, the video playback reaches a second section, the corresponding key for that section is transmitted to the customer and the key for the previous section is destroyed.
>
> (Emphasis added)

The Examiner has completely ignored the clear and definite use of the terms "current" and "next" in the execution of the flowchart shown in Figure 3 of the instant application. The Examiner's suggested interpretation of Figure 3 completely ignores the actual operation of the method illustrated in the flowchart.

In order to further emphasize the operation of the method illustrated in the flowchart of Figure 3, the following example execution of the flowchart for encrypted video data content that includes three encrypted sections is provided. This example is provided for illustrative purposes only, and is only meant to highlight the clear and evident teachings of Figure 3.

For illustrative purposes, we will call the encrypted sections SECTION 1, SECTION 2 and SECTION 3 having respective decryption keys KEY 1, KEY 2 and KEY 3 and it will be assumed that the customer processing platform has previously downloaded the three encrypted sections of video data content (See page 19, lines 1-2) and steps 31 to 36 of Figure 3 have been executed. That is, the customer processing platform has possession of the three encrypted sections SECTION 1, SECTION 2 and SECTION 3. At step 37, KEY 1, i.e. the respective decryption key in respect of the "current" encrypted section (SECTION 1), is delivered to the customer processing platform. The customer begins to decrypt and view SECTION 1 with KEY 1 in step 38. Because SECTION 1 is not the last section, in step 39 the method proceeds to step 41. In step 41, KEY 2, i.e. the respective decryption key in respect of the "next" encrypted section (SECTION 2) is delivered to the customer processing platform. Clearly at this point the customer processing platform has received the respective decryption key (KEY 2) in respect of the next encrypted section (SECTION 2). The method then enters the "holding pattern" of steps 42 and 43 until SECTION 1 is finished. In step 44, KEY 1 is destroyed and the next encrypted section (SECTION 2) is decrypted and viewed using KEY 2 (See page 20, lines 5 to 7). Clearly KEY 1 is destroyed in step 44 after KEY 2 is received in step 41. At this point, the method returns to step 39, in which SECTION 2 is now considered the "current section" and SECTION 3 is now considered the "next section". Because SECTION 2 is not the "last" section, the method proceeds to step 41. In step 41, KEY 3 is delivered to the customer processing platform and the "holding pattern" of steps 42 and 43 is entered into until SECTION 2, i.e. the "current" section, is finished. Once SECTION 2 is finished, KEY 2 is destroyed in step 44, which is clearly after the respective decryption key (KEY 3) for the next encrypted section (SECTION 3) was delivered in step 41, and the next encrypted section (SECTION 3) is decrypted and viewed using KEY 3. Because SECTION 3 is the last section of encrypted video data content in this example, when the method returns to step 39 it will proceed to the END in step 40.

Applicant respectfully submits that the foregoing example clearly illustrates the proper understanding and operation of the flowchart shown in Figure 3 and completely precludes the Examiner's nonsensical misinterpretation of the Figure.

It is noted that in the Final Action dated March 10, 2010 the Examiner provides absolutely no basis for the assertion that the foregoing features of the claims are not supported in the originally filed application. Moreover, the Examiner fails to provide an explanation of what Figure 3 does in fact show, if it does not show what Applicant asserts that it does. During the telephone conversation with the Examiner on June 4, 2010, the Examiner suggested that Figure 3 shows that the key for a current section is deleted before the key for the next section is received.

However, as demonstrated above, this type of interpretation is completely unsupportable by Figure 3 and its accompanying description.

Accordingly, Applicant respectfully submits that the Examiner's rejection under 35 U.S.C. 112, first paragraph should be reconsidered and withdrawn. Furthermore, as Applicant has addressed the Examiner's rejection under 35 U.S.C. 112, first paragraph, it is Applicant's understanding that the application should now be considered allowable, as the Examiner's remarks in the Examiner-initiated telephone interview on March 4, 2010 indicated that the Examiner was prepared to allow the application if Applicant were to identify some portion of the application that provides support for the language of claims 16, 34 and 54. Nonetheless, the rejections raised in the Final Rejection dated June 22, 2009, which were first addressed in Applicant's Appeal Brief dated December 10, 2009, and which are reasserted in the Final Rejection dated March 20, 2010, are addressed again below in their entirety.

35 U.S.C. 112, Second Paragraph

2. Whether claims 16-23, 34 and 54-56 are unpatentable under 35 U.S.C. 112, second paragraph.

In paragraph 12 of the Final Action dated June 22, 2009, and again in paragraph 17 of the Final Action dated March 10, 2010, the Examiner rejects claims 16 and 34 under 35 U.S.C. 112, second paragraph on the grounds that "it would be unclear to one or ordinary skill in the art to understand which of the preceding blocks or sections of the plurality of the encrypted blocks or sections that will be completed before the next keys is received" (emphasis added). The Examiner seems to have interpreted claims 16 and 34 to recite that a decryption key for a next encrypted section is only received after decryption of a preceding encrypted section is completed. This is entirely contrary to the actual recited subject matter of the claims. For example, independent claim 16 clearly recites in part "for each encrypted section: receiving a respective decryption key in respect of the encrypted section before playback of a preceding encrypted section of the plurality of encrypted sections is complete;" (emphasis added).

Furthermore, Applicant respectfully submits that when the claim is read as a whole a person of ordinary skill in the art would readily understand that the claim encompasses receiving (claims 16) and transmitting (claim 34) decryption keys for a next encrypted section before playback of any one of the preceding encrypted sections is completed to facilitate contiguous playback of the encrypted video content. In some embodiments this may be an immediately preceding encrypted section, such that a decryption key in respect of a next encrypted section of encrypted video content is delivered before playback of the encrypted section that immediately precedes the next encrypted section is completed. In other embodiments, the decryption key in respect of the next encrypted section is delivered before playback of an earlier encrypted section (prior to the immediately preceding encrypted section) is completed. Also, when the claim is read as a whole a person of ordinary skill in the art would readily understand that the destruction of decryption keys at the customer processing platform, as recited in the claims, is carried out such that at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content. Accordingly, Applicant respectfully submits that the rejection under 35 U.S.C. 112, second paragraph of independent claims 16 and 34, and the dependent claims that depend therefrom, should be withdrawn.

35 U.S.C. 103(a)

The following arguments relate to rejections raised by the Examiner under 35 U.S.C. 103. The law on obviousness under 35 U.S.C. 103 was addressed by the United States Supreme Court in ***KSR Int'l v. Teleflex, Inc.***, 127 S.Ct. 1727, 1741 (2007). Following this, examination guidelines were released on October 10, 2007 in regards to determining obviousness under 35 U.S.C. 103. According to these guidelines, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in ***Graham v. John Deere Co****. 383 U.S. 1,148 USPQ 459 (1966)*. Obviousness is a question of law based on underlying factual inquiries. The factual inquiries enunciated by the Court are as follows:

(1) Determining the scope and content of the prior art;

(2) Ascertaining the differences between the claimed invention and the prior art; and

(3) Resolving the level of ordinary skill in the pertinent art.

The Graham factors, including secondary considerations when present, are the controlling inquiries in any obviousness analysis. Once the findings of fact are articulated, Office personnel must provide an explanation to support an obviousness rejection under 35 U.S.C. 103. According to the Supreme Court ruling in ***KSR***, for the Patent Office to properly combine references in support of an obviousness rejection, the Patent Office must identify a reason why a person of ordinary skill in the art would have sought to combine the respective teachings of the applied references.

In rejecting claims under 35 U.S.C. § 103(a), the Examiner bears the initial burden of establishing a prima facie case of obviousness. ***In re Oetiker***, 977 F.2d 1443, 1445 (Fed. Cir. 1992). See also ***In re Piasecki***, 745 F.2d 1468, 1472 (Fed. Cir. 1984). It is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See* ***In re Fine***, 837 F.2d, 1071, 1073 (Fed. Cir. 1988). In so doing, the examiner is expected to make the factual determinations set forth in ***Graham v. John Deere Co.***, 383 U.S. 1, 17 (1966), *viz.*, (1) the scope and content of the prior art; (2) the differences between the prior art and the claims at issue; and (3) the level of ordinary skill in the art. Additionally, in making a rejection under 35 U.S.C. § 103(a) on the basis of obviousness, the Examiner must provide some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. ***KSR Int'l. Co. v. Teleflex Inc.***,127 S.Ct. 1727, 1741 (2007). Only if this initial burden is met does the burden of coming forward with evidence or argument shift to the appellant. See ***Oetiker***, 977 F.2d at 1445. See also ***Piasecki***, 745 F.2d at 1472. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. See ***Oetiker***, 977 F.2d at 1445; ***Piasecki***, 745 F.2d at 1472.

Applicant's analysis below demonstrates that the Examiner's rejections under 35 U.S.C. 103(a) should be withdrawn, as an analysis following the factual inquiries laid out in ***Graham v. John Deere Co.*** clearly reveals errors in the Examiner's rejections raised under 35 U.S.C. 103(a).

3. Whether claims 16-18, 21, 54 and 55 are unpatentable under 35 U.S.C. 103(a) over Feig et al. (U.S. Patent No. 7,251,833 B2) in view of Giroux et al. (U.S. Patent Application Publication No. 2002/0078361 A1).

Determining The Scope Of The Prior Art

Feig et al.

Feig et al. describes a method for enforcing the sequential playback of a multimedia file by partitioning the media file into a plurality of sequential data blocks, encoding each respective one of the sequential data blocks with a corresponding one of a plurality of encryption keys, transferring the encoded sequential data blocks to a receiving client, and streaming a plurality of decryption keys to the receiving client.

Feig et al. teaches that the decryption keys are streamed one at a time to the client to enforce sequential playback of the media file, but fails to describe any mechanism for preventing the client from retaining all of the decryption keys and all of the decrypted content once all of the decryption keys have been delivered to the client.

The Examiner has pointed to Figure 3 (steps 308-314), column 2, lines 40-65 and column 3 lines 1-5 of Feig et al. in support of the allegation that Feig et al. discloses "delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time". However, by the Examiner's own admission, these portions of Feig et al., and Feig et al. as a whole, merely teach that:

> "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one-to-one decryption and playback of the encrypted sequential data blocks"; and
>
> "[the] preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys ... and for playing back each recovered sequential data".

Applicant respectfully submits that the Examiner's own statements clearly demonstrate that Feig et al. merely discloses the sequential streaming of token keys to a client receiver and the decryption of encrypted content using the streamed token keys. There is no suggestion whatsoever in Feig et al. that each decryption key is delivered and then deleted or destroyed after decryption of the corresponding encrypted content segment in a manner that would prevent the client from simultaneously having possession of all of the decryption keys. In fact, Feig et al. clearly states that token keys (decryption keys) are retained by the customers once they are delivered. For example, column 2, lines 56 to 58 states that "all of the cryptographic token keys may also be transmitted to the client receiver as a single block of data for storage and later use" (emphasis added).

Giroux et al.

Giroux et al. teaches an information security architecture for encrypting and distributing a segment of electronic information for remote access while maintaining access control to the encrypted electronic information by dispensing decryption keys for the encrypted electronic information via a remote server 106 to an authorized user 116, and causing the user's decryption tool (viewing tool 104) to delete/destroy the decryption key after the encrypted segment of electronic information is decrypted. The decrypted electronic information is also destroyed once it is displayed on the viewing tool 104. It is important to note that Giroux et al. teaches that a next decryption key for a next encrypted segment of electronic information is not delivered to a customer until customer requests the next decryption key after the decryption of the current encrypted segment is completed, the decrypted information is displayed and the current decryption key has been deleted. See paragraph [0051], which states:

> "If the user 216 is authorized to access the section, the server 206 sends the decryption key and options for that section to the Application Utility 230 at the viewing user's computer 224 and the Application Utility 230 decrypts the section using the decryption key. After decrypting the section, the Application Utility 230 immediately discards/destroys the key, loads the decrypted section into the display buffers to render the decrypted section to the screen, and then clears the buffers to destroy the decrypted version of the section. When the viewing user moves to a different section, the process is repeated." (Emphasis added)

Effectively, Giroux et al. prevents the customer from simultaneously having possession of more than a single decryption key. If the method taught by Giroux et al. were applied to video content, the customer would not receive the decryption key to decrypt the next segment of encrypted video content until after the previous segment was decrypted, displayed and deleted along with the previous decryption key. This would effectively prevent uninterrupted viewing of video content, as there would be some delay when the Application utility 230 "clears the buffers to destroy the decrypted version of the section" and then has to repeat the decryption key request to receive the next decryption key.

Ascertaining The Differences Between The Prior Art And The Claims At Issue

Independent Claim 16

Previously presented independent claim 16, as amended in the Office Action response dated August 1, 2008, recited destroying the decryption key for each encrypted section of data content only after at least the decryption key in respect of the next encrypted section has been received, such that at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of data content. It is important to note that this feature means that the customer processing platform will have possession of the decryption key for the current encrypted section and the decryption key for the next encrypted section. This allows the seamless playback of the encrypted data content, since the customer processing platform is able to retrieve the decryption key for the next encrypted section before playback of the preceding encrypted section is complete.

In order to clarify this operation, claim 16 was amended in the Office Action response dated February 13, 2009 to recite:

> 16. A method of receiving and controlling playback of video data content at a customer processing platform, comprising:

receiving over a communications medium a plurality of encrypted sections of video data content, each of which has been encrypted using a respective encryption key; and

for each encrypted section:

receiving a respective decryption key in respect of the encrypted section before playback of a preceding encrypted section is complete;

decrypting and playing back the encrypted section using the respective decryption key; and

destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data content is provided **and** at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content. (emphasis added)

The Examiner has acknowledged that Feig et al. is entirely silent with respect to the destruction of decryption keys. As such, all of the teachings of Feig et al. result in a customer receiving and maintaining a complete set of decryption keys for a given piece of encrypted content. In Applicant's response filed February 13, 2009, Applicant argued that Feig et al. fails to teach or even suggest "for each encrypted section: receiving a respective decryption key in respect of the encrypted section before playback of a preceding encrypted section of the plurality of encrypted sections is complete", as recited in claim 16. In response this argument by the Applicant, in the Final Action dated June 22, 2009 and again in the Final Action dated March 10, 2010, the Examiner points to the embodiment described in Feig et al. in which "the server 100 would transmit all of the token keys in a token key block, wherein each respective token key can be retrieved from the token key block at the client receiver 200 in a sequence ordered by the order of occurrence of playback of each corresponding one of the partitioned multimedia file 102" (See paragraph 3 of the final rejection; emphasis added). Applicant respectfully submits that it is important to realize that the embodiment of Feig et al. to which the Examiner is referring obviously includes the delivery of all of the token keys necessary to decrypt a multimedia file to a client receiver 200, so that the client receiver 200 has simultaneous possession of all of the token keys necessary to decrypt the multimedia file, **which is entirely contrary to the claimed invention**.

The Examiner has relied on Giroux et al. for allegedly teaching the destruction of decryption keys. However, Giroux et al. fails to teach or even suggest the destruction of decryption keys in accordance with Applicant's claims. Specifically, Giroux et al. requires two conditions be satisfied before a decryption key for a next encrypted section of data content is requested by a customer:

a) the decryption key for a current encrypted section is destroyed following decryption and/or display of the content of the current encrypted section; and

b) the display buffers, which the decrypted data content from the current encrypted section were loaded into, are cleared following display of the content.

Giroux et al. is intended for data contents which are not time sensitive, such as written documents. Although Giroux et al. does make reference to audio clips and video clips, it should be understood that Giroux et al. is clearly not directed to the sequential playback of sequential contiguous audio clips or video clips, as the content control processes according to Giroux et al. would prevent the seamless playback of such content. It is clear that the main thrust of Giroux et al. is to written documents, for example, see Giroux et al. [0002], which states "Electronic security systems have been proposed for managing access to electronic information and electronic documents so that only authorized users may open protected information and documents. Several software tools have been developed to work with particular document readers such as Adobe Acrobat Exchange and Adobe Acrobat Reader".

In Giroux et al., the intention of encrypting different sections of a document with different keys is to be able to control which users have access to which subsets of the document.

See, for example, Giroux et al. [0014], which states "… The document or information may also be broken down into sections using the authoring tool 102, so that certain sections within a document may have different keys and/or access policies. For example, a set of users may be allowed to view pages 1-5 of a 10-page document, while a subset of those users may be allowed to view all 10 pages of the document."

Although Giroux et al. does briefly mention that the techniques described therein could be used for music and video applications, Giroux et al. provides absolutely no teaching of how the delivery, use and deletion of decryption keys would be handled in such applications. Given the fact that all of the substantive teachings of Giroux et al. relate to the encryption of discrete chapters of a non-time-sensitive document with respective encryption keys, Applicant respectfully submits that one skilled in the art would understand that the references to "music" and "video" applications in Giroux et al. pertain to applications in which independent and non-contiguous pieces of music and video content are encrypted with respective encryption keys and their individual and non-contiguous playback is controlled by the decryption key access procedure described in Giroux et al. For example, one skilled in the art would understand that the reference to "music" applications in Giroux et al. pertains to the encryption of each individual song of a record with a respective encryption key, such that non-contiguous playback of the individual songs is governed by the decryption key access procedure described in Giroux et al. Similarly, encryption and decryption of a sequence of non-contiguous video files with respective encryption/decryption keys may be contemplated by Giroux et al., but certainly not that of contiguous video data, as none of the teachings of Giroux et al. are capable of supporting such operation.

It should be clear that Giroux et al. is not in any way directed to providing seamless playback of sequential contiguous sections of encrypted video data content, rather Giroux et al. is directed to controlling access to discrete sections of data content in a non-time-sensitive manner. See, for example, Giroux et al. [0016], which states "Viewing tool 104 loads the resulting clear text into the display buffers to render the document section on a display, destroys the decrypted key, and clears the display buffers to destroy the clear text version of the document section. The clear text will thus be visible on the display, but will not exist in electronic form in a manner that can be copied or manipulated." See also Giroux et al. [0051], which states " … If the user 216 is authorized to access the section, the server 206 sends the decryption key and options for that section to the Application Utility 230 at the viewing user's computer 224 and the Application Utility 230 decrypts the section using the decryption key. After decrypting the section, the Application Utility 230 immediately discards/destroys the key, loads the decrypted section into the display buffers to render the decrypted section to the screen, and then clears the buffers to destroy the decrypted version of the section. When the viewing user moves to a different section, the process is repeated." It should be clear that the phrase "when the viewing user moves to a different section, the process is repeated", requires that the request for access to the "different section" be transmitted to server 206 in order to receive the decryption key for the "different section", and that according to Giroux et al., this request is only generated after the viewing user attempts to "move to a different section", i.e., only after the data for the current section has been decrypted, the current decryption key is destroyed, the decrypted data is loaded into the display buffers, rendered on the screen and subsequently cleared from the buffers. In other words, Giroux et al. does not allow the viewing user to receive the decryption key for the "different section" until after the viewing user has finished viewing the current section.

In contrast, in accordance with claim 16, the decryption key for a second encrypted section of video data content is received before playback of the first encrypted section of video data content is complete, and that the decryption key for the first encrypted section is not deleted until after at least the decryption key for the second encrypted section is received, which means that the customer processing platform is able to obtain the decryption key for the second encrypted section before playback of the first encrypted section is complete, e.g. before the decrypted content of the first encrypted section is completely displayed to a viewing user, so that the customer processing platform can begin decryption of the second encrypted section before playback of the first encrypted section is complete. This then potentially allows for the seamless playback of sequential time-sensitive video data content in a manner that could not be realized by an unimaginative person of ordinary skill in the art having regard to Feig et al. and Giroux et al.

Independent claim 16 recites a method of receiving and controlling playback of video data content at a customer processing platform, which involves streaming decryption keys to the customer processing platform in a manner that facilitates contiguous playback of the encrypted video data content and deleting the decryption keys in a manner such that at any time the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys necessary to decrypt the encrypted video data content.

It must be appreciated that there are three inter-related procedures that are involved in the claimed invention: reception of a decryption key, decryption of an encrypted section of video data content corresponding to the decryption key, and the destruction of the decryption key, with the three procedures carried out in the claimed manner to allow contiguous playback of the encrypted video data content and to prevent the customer processing platform from having simultaneous possession of all of the decryption keys for decrypting the video data content. Neither Feig et al. nor Giroux et al. contemplates this type of operation, and Applicant respectfully submits that the Examiner's suggested combination of the cited references is based solely on a reading of the references with hindsight analysis using the instant application as a template.

It should be further appreciated that the teachings of Feig et al. to which the Examiner points in support of the rejection of claims 16 and 34, in so far as those teachings refer to the delivery of an entire set of token keys to a client receiver, are entirely incompatible with the teachings of Giroux et al., in so far as the teachings of Giroux et al. are directed to the delivery of a decryption key for a different piece of encrypted data content only after a previously used key is destroyed and the data decrypted with the previously used key has been deleted from memory.

Furthermore, Applicant submits that in light of the foregoing incompatibility of the cited references the Examiner's attempts to combine these references to arrive at the present invention is obviously an attempt to reconstruct the claimed invention using the instant application as a template. The Examiner totally ignores this incompatibility, despite the fact that the teachings of Feig et al. that the Examiner has pointed to in paragraph 3 of the final rejection for allegedly teaching "for each encrypted section: receiving a respective decryption key in respect of the encrypted section <u>before playback of a preceding encrypted section of the plurality of encrypted sections is complete</u>", as recited in claim 16, <u>requires advance delivery of all of the</u>

decryption keys to the client receiver.

In the response filed February 13, 2009, Applicant argued that Giroux et al. fails to teach or even suggest "destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received", as recited in claim 16. In response to Applicant's argument, in paragraph 4 of the Final Action the Examiner states that Applicant's argument is "against the references individually" and cautions that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references". However, the Examiner has explicitly acknowledged that Feig et al. is silent with respect to the destruction of decryption keys, and relies solely on Giroux et al. for this feature. Accordingly, Applicant's assertions regarding the deficiencies in the teachings of Giroux et al. is appropriate.

Applicant respectfully submits that no combination of the cited portions of Feig et al. and Giroux et al. can be found to render claim 16 obvious, as the cited portions of Feig et al. that the Examiner relies on for providing contiguous playback of the encrypted sections of video content teaches that all of the decryption keys must be sent to the customer receiver so that the customer receiver has simultaneous possession of all of the decryption keys, and the cited portions of Giroux et al. that the Examiner relies on for providing destruction of decryption keys precludes contiguous playback, since it requires the destruction of a previous decryption key and the deletion of decrypted content from memory prior to delivery of a decryption key in respect of a different portion of encrypted data content.

In paragraph 17 on page 10 of the Final Action dated June 22, 2009, and again in paragraph 22 of the Final Action dated March 10, 2010, the Examiner asserts that "it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al. and incorporate the method of destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content in view of the teachings of Giroux et al." (emphasis added). However, as noted in Applicant's Office

Action response dated February 13, 2009, and discussed above with reference to paragraph [0051] of Giroux et al., the underlined portion of this assertion is clearly inaccurate, as the content access control methods described in Giroux et al. require that the customer request the decryption key for the "next section" only after the decryption key for the previous section is destroyed and the decrypted data from the display buffers has been cleared. As such, one skilled in the art would find no teaching in Giroux et al. of "destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received", as this feature is completely contrary to all of the teachings of Giroux et al.

In rejecting claim 16, the Examiner alleges that the claimed invention, as recited in claims 16 "is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable" (paragraph 17 of Final Action dated June 22, 2009 and paragraph 22 of Final Action dated March 10, 2010; emphasis added). However, Applicant has demonstrated above that the claimed invention is not merely a combination of old elements, rather the claimed invention includes methods having decryption key delivery, use and destruction steps that provide a technical solution unrecognized and unresolved by either of the cited references, when considered alone and in combination, thereby providing a non-obvious result.

In addition, Applicant respectfully submits that one skilled in the art would find no reason to look to Giroux et al., in so far as Giroux et al. is solely directed to controlling access to particular portions of non-time-sensitive documents and disparate non-contiguous audio/video clips, when attempting to modify the teachings of Feig et al., which are solely directed to enforcing the sequential playback of a contiguous video encrypted with a plurality of encryption keys. This is further reinforced by the fact that there is absolutely no recognition of the piracy problem associated with the time-sensitive streaming of decryption keys for playback of encrypted sections of video data content, which Applicant's claimed invention aims to address. Even if Giroux et al. does teach the destruction of decryption keys at a user's data processing device, Giroux et al. fails to teach or even suggest a manner in which the decryption keys can be delivered, used and then destroyed such that time-sensitive playback of a plurality of encrypted sections of a contiguous video is possible. In fact there is absolutely no suggestion in either of the references that such a problem exists, i.e., there is no recognition in the cited references of the problems associated with providing contiguous playback of a video while also mitigating piracy of the video.

In view of the foregoing, Applicant respectfully submits that the Examiner's suggested motivation for combining the teachings of Feig et al. and Giroux et al. is not based on an objective analysis of the cited references, but is instead the result of an attempt to reconstruct the claimed invention by picking and choosing elements from the cited references, while using the application as a template, which is completely impermissible—see ***In re Fine***, 837 F.3d 1071 (Fed. Cir. 1988).

Accordingly, Applicant respectfully submits that the rejection of independent claim 16 under 35 U.S.C. 103(a) in view of Giroux et al. and Feig et al. should be reconsidered and withdrawn.

Dependent Claims 17-18, 21, 54 and 55

Based at least on their dependence from independent claim 16, Applicant respectfully submits that the rejection of dependent claims 17-18, 21 and 54-55 under 35 U.S.C. 103(a) should be reconsidered and withdrawn for at least the same reasons as the rejection of independent claim 16.

Furthermore, with respect to dependent claim 54, Applicant respectfully submits that Feig et al. and Giroux et al. fail to teach or even suggest "wherein destroying the respective decryption key only after at least the respective decryption key in respect of the next encrypted section has been received comprises destroying the respective decryption key only after completing playback of the encrypted section **and** beginning contiguous playback of the next encrypted section" as recited in claim 54 (emphasis added). In support of the rejection of claim 54 in paragraph 25 on page 14 of the Final Action dated March 10, 2010, the Examiner asserts that Giroux et al. teaches the foregoing feature of claim 54. In support of this assertion the Examiner points to paragraph [0051] of Giroux et al. However, as noted above, paragraph [0051] of Giroux et al. clearly describes a process by which a decryption key is requested for a current section of encrypted content, the decryption key is used and then the decrypted content and the decryption key are destroyed before a further request for another key is even made. Accordingly, the Examiner's assertion is clearly totally erroneous, as Giroux et al. clearly does not teach or even suggest destroying a decryption key for a given section of encrypted content only after playback has of the encrypted section has completed and contiguous playback of the next encrypted section has begun.

In addition, with respect to dependent claim 55, Applicant respectfully submits that Feig et al. and Giroux et al. fail to teach or even suggest "for each encrypted section: requesting the respective decryption key in respect of a next encrypted section responsive to one of a control signal and a data pattern in the decrypted data content of an encrypted section that precedes the next encrypted section.", as recited in claim 55 (emphasis added). In support of the rejection of claim 55 under 35 U.S.C. 103(a) the Examiner asserts that Feig et al. teaches the foregoing feature of claim 55. In support of this assertion the Examiner points to column 8, lines 1-15 of Feig et al. However, Applicant respectfully submits that the teachings at column 8, lines 1-15 of Feig et al. are completely silent with respect to the foregoing feature of claim 55. Column 7, lines 66 to Column 8, line 15 of Feig et al. is quoted below for ease of reference.

> In order to control the time and sequence of viewing of the content of the multimedia file 102 at the client receiver 200, sequence numbers can be included in the token keys so that only after all of the token keys are received can any viewing take place. Such an embedded sequence value in each token key will govern or enforce the sequential playback of each respective multimedia minute block 1, 2, 3, etc. In other words, the server 100 would transmit all of the token keys in a token key block, wherein each respective token key can be retrieved from the token key block at the client receiver 200 in a sequence ordered by the order of occurrence of playback of each corresponding one of the partitioned multimedia file 102. This order of occurrence would be enforced by the embedding of the sequence number in each respective token. Thus, each token must be applied to the data block decoder 54 in the numerically increasing order of its embedded sequence number. (Emphasis added)

With reference to the foregoing quoted portion of Feig et al. it should be immediately clear that it relates to the embedding of sequence numbers in the token keys (decryption keys), whereas claim 55 recites "requesting the respective decryption key in respect of a next encrypted section responsive to one of a control signal and a data pattern **in the decrypted data content** of an encrypted section that precedes the next encrypted section". Applicant respectfully submits that it is entirely inappropriate to equate sequence numbers embedded in token keys, as taught by Feig et al., with a control signal or a data pattern in decrypted data content. In fact, the cited portion of Feig et al. merely states that token keys can be retrieved from the token key block (which contains all of the token keys at the customer's receiver) in a sequence ordered by the order of occurrence of playback of each corresponding encrypted section. Applicant respectfully submits that the cited portion of Feig et al. is entirely silent with respect to making a request for a next key responsive to the embedded sequence numbers, let alone responsive to one of a control signal and a data pattern in the decrypted data content, as recited in claim 55.

Furthermore, please note that the section of Feig et al. that the Examiner has pointed to in support of the rejection of claim 55 explicitly states that "only after all of the token keys are received can any viewing take place", i.e. the customer has simultaneous possession of all of the token keys, which is entirely contrary to claimed invention.

In view of the foregoing, Applicant respectfully submits that the rejection of claims 16-18, 21 and 54-55 under 35 U.S.C. 103(a) should be reconsidered and withdrawn.

4. Whether claim 19 is unpatentable under 35 U.S.C. 103(a) over Feig et al. in view of Giroux et al. and further in view of Granger et al. (U.S. Patent No. 6,334,189 B1)

Determining The Scope Of The Prior Art

Feig et al. and Giroux et al. are discussed above with reference to independent claim 16, therefore a discussion of the scope of their teachings is not repeated here.

Granger et al.

Granger et al. describes three methods for protecting software applications from unauthorized distribution and use. The first method involves using values generated by a conventional ESD (Electronic Security Device) to encrypt and/or decrypt user data (such as a file) that is generated and used by the application. In one embodiment, the user data is encrypted using values returned by the ESD, and the user data is later decrypted using like values returned by a software-implemented ESD simulator. The second and third methods involve the use of special development tools in an effort to make the task of analyzing the application's copy protection code (such as the code used to encrypt and/or decrypt user data) more difficult. Specifically, the second method involves using pseudocode to implement some or all of the application's copy protection functions. The pseudocode for a given function is generated from actual code using a special development tool, and is then imbedded within the application together with a corresponding pseudocode interpreter. The interpreter fetches, decrypts and executes the pseudocode when the function is called. The third method involves the use of an obfuscation tool to convert the code for selected copy-protection functions into long, inefficient sequences of machine code.

The Examiner has specifically pointed to Figures 1A and 1B of Granger et al. In Figures 1A/1B of Granger et al., a seed value is provided to an ESD/ESD Simulator to generate an encryption/decryption key to encrypt/decrypt user data. It is important to note that the ESD/ESD simulator creates the encryption/decryption key based only on the seed value. The encryption/decryption key is not based in any way on user-specific information.

Ascertaining The Differences Between The Prior Art And The Claims At Issue

Applicant respectfully submits that Granger fails to overcome any of the deficiencies of Feig et al. and Giroux et al., which are discussed above with reference to independent claim 16.

By virtue of its claim dependency on independent claim 16, Applicant respectfully submits that the rejection of dependent claim 19 should be reconsidered and withdrawn for at least the same reasons as the rejection of independent claim 16.

5. Whether claims 22 and 23 are unpatentable under 35 U.S.C. 103(a) over Feig et al. in view of Giroux et al. and further in view of Watanabe et al. (U.S. Patent No. 7,114,073 B2)

Determining The Scope Of The Prior Art

Feig et al. and Giroux et al. are discussed above with reference to independent claim 16, therefore a discussion of the scope of their teachings is not repeated here.

Watanabe

Watanabe describes a digital contents generating apparatus connected with a communication network that includes an electronic watermark-data embedding unit for embedding electronic watermark data in digital contents, an encryption unit for encrypting the digital contents embedded with electronic watermark data by an encryption key received from an encryption-key generating unit, and a decryption-key generating unit for generating a decryption key. A digital contents reproducing apparatus connected with the communication network includes an electronic watermark data extraction unit for extracting electronic watermark data from encrypted digital contents embedded with electronic watermark data, and a decryption unit for decrypting the encrypted digital contents using a predetermined decryption key.

In one of the examples described in Watanabe, the encryption-key generating unit generates an encryption key based in part on the IP address of a user to whom the digital content is to be transmitted (See column 5, lines 17 to 35).

Ascertaining The Differences Between The Prior Art And The Claims At Issue

Applicant respectfully submits that Watanabe fails to overcome any of the deficiencies of Feig et al. and Giroux et al., which are discussed above with reference to independent claim 16.

By virtue of their dependence from independent claim 16, Applicant respectfully submits that the rejection of dependent claims 22 and 23 should be reconsidered and withdrawn for at least the same reasons as the rejection of independent claim 16.

6. Whether claim 20 is unpatentable under 35 U.S.C. 103(a) over Feig et al. in view of Giroux et al. and further in view of Novak (U.S. Patent Application Publication No. 2003/0097655)

Determining The Scope Of The Prior Art

Feig et al. and Giroux et al. are discussed above with reference to independent claim 16, therefore a discussion of the scope of their teachings is not repeated here.

Novak

Novak describes a system and method for providing conditional access to digital content in which in response to a user request to view specific digital content, the user's set top box (STB) accesses a verification entity via a persistent network connection. The STB establishes the user's identity with the verification entity, for instance, by reading identity credentials from a smart card. In response to the verification entity having stored a license for the user to view the digital content, the STB receives a license key from the verification entity. In addition, the STB receives an encrypted access key from an access key source corresponding to a segment of encrypted digital content. The license key is used to decrypt the encrypted access key, which is, in turn, used to decrypt the segment of encrypted digital content. A user may transfer his or her license in whole or in part to another user by sending a transfer request to the verification entity.

Ascertaining The Differences Between The Prior Art And The Claims At Issue

Applicant respectfully submits that Novak fails to overcome any of the deficiencies of Feig et al. and Giroux et al., which are discussed above with reference to independent claim 16.

By virtue of its dependence from independent claim 16, Applicant respectfully submits that the rejection of dependent claim 20 should be reconsidered and withdrawn for at least the same reasons as the rejection of independent claim 16.

7. Whether claims 34 and 56 are unpatentable under 35 U.S.C. 103(a) over Peterka (U.S. Patent Application Publication No. 2002/0170053) in view of Feig et al. and further in view of Giroux et al.

Peterka et al.

Peterka et al. describes a method for distributing encrypted data content which uses a hierarchy of encryption keys to provide for flexible billing options. Specifically, Peterka et al. describes a Pay-By-Time (PBT) billing option (See [0048]) in which a program is segmented into a plurality of program segments. The actual data of each respective program segment is then encrypted with at least one respective content key (CK). The respective content keys are then each encrypted with a respective program segment key (PSK). When a consumer wishes to join a multicast of the program, the consumer contacts an Origin Content Server (OCS) to begin receiving PSKs. The PSKs are distributed to the consumer in a multicast in which the PSKs are encrypted with the consumer's unique key (UK).

In order to actually view a program segment, the consumer must first decrypt the PSK corresponding to that program segment with the consumer's UK, then use that decrypted PSK to decrypt the CK corresponding to that program segment and then finally decrypt that program segment with the decrypted CK. In the Pay-By-Time billing method, the consumer must continue to request each new PSK in order to continue viewing the program, i.e. to continue decrypting program segments. Peterka also teaches that the content key for a future program segment may be encrypted with not only the PSK corresponding to the future program segment, but also with an old PSK of an old program segment. "Thus, if a user has not yet received a new program segment key, the content key can be obtained by utilizing the old program segment key." (see [0109] and Figure 9). Furthermore, Peterka et al. teaches that the content keys are maintained by the consumers, for possible use in later decryption. For example, Peterka describes a signalling method in which "a predetermined bit can be used to indicate if an **old or current content key should be used as opposed to a new content key** which has recently been distributed to the client." (see [0119]; emphasis added)

Feig et al. and Giroux et al. are discussed above with reference to independent claim 16, therefore a discussion of the scope of their teachings is not repeated here.

Ascertaining The Differences Between The Prior Art And The Claims At Issue

Independent Claim 34

Independent claim 34 recites:

> 34. A method for controlling use of encrypted video data content downloaded to a customer data content processing device, comprising:
>
> receiving a request comprising customer verification information from a customer data content processing device;
>
> comparing the customer verification information with corresponding stored customer information; and
>
> where the customer verification information is consistent with the stored customer verification information:
>
> billing a usage charge to an account of the customer;
>
> transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted video data content; and
>
> for each subsequent portion of the encrypted video data content:
>
> transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted video data content before playback of a preceding portion of the encrypted video data content is complete; and
>
> causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device only after at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device, such that contiguous playback of the

> portions of encrypted video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted video data content. (emphasis added)

In paragraph 31 of the Final Action, the Examiner acknowledges that Peterka et al. fails to disclose:

> "for each subsequent portion of the encrypted video data content:
>
> transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted video data content before playback of a preceding portion of the encrypted video data content is complete; and
>
> causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device only after at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device, such that contiguous playback of the portions of encrypted video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted video data content."

In support of the rejection of claim 34, the Examiner has asserted that Feig et al. and Giroux et al., when combined, teach the foregoing features of claim 34 that the Examiner acknowledges are not disclosed by Peterka et al. Applicant disagrees with this assertion.

In the teachings of both Peterka et al. and Feig et al. the customer **retains possession** of the decryption keys and the decrypted content, i.e., by the end of a program (end of decryption of last encrypted program segment), the customer has all of the decrypted content and the full set of decryption keys, thereby allowing unrestricted access/use of the decrypted content. The customer could then potentially copy and distribute the decrypted content and/or the decryption keys and encrypted content.

In paragraph 38 of the Final Action dated March 10, 2010, the Examiner asserts that Giroux et al. "discloses a method of causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device only after at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device, such that contiguous playback of the portions of encrypted video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted video data content". (Emphasis added) However, Applicant respectfully submits that Giroux et al. fails to teach or even suggest any such feature, and furthermore submits that the portion of Giroux et al. to which the Examiner points in support of the foregoing assertion is completely contradictory to the Examiner's assertion.

In support of the foregoing assertion regarding Giroux et al. in paragraph 38 of the Final Action, the Examiner points to paragraph [0051] of Giroux et al., which, as noted above with respect to the Examiner's rejection of independent claim 16, teaches that a next decryption key is not delivered to a customer until the previous decryption key has been deleted and the decrypted content of the previous encrypted segment has been displayed and deleted. That is, in accordance with the decryption key destruction process described in Giroux et al., the customer only ever has possession of a single decryption key at a time.

In contrast, independent claim 34 recites delivery of a current decryption key and the next decryption key to a customer processing platform and the destroying of the current key only after at least the next key has been received. This feature of independent claim 34 allows the buffering of encrypted sections of data content and a subset of the plurality of decryption keys to decrypt the encrypted sections, so that decryption and playback of the data content can be seemless and uninterrupted. It should be noted that independent claim 34 covers embodiments in which, for example, the first decryption key of the plurality of decryption keys is destroyed at any time after at least the second decryption key has been received. For example, independent claim 34 covers the following scenarios:

a) the customer processing platform receives the first decryption key and the second decryption key and deletes the first decryption key when decryption of the first encrypted section is completed and decryption of the second encrypted section has begun. (e.g. the first decryption key is deleted before the third decryption key is received, such that the customer processing platform only ever has simultaneous possession of two decryption keys); and

b) the customer processing platform receives a current decryption key and any subset of the remaining decryption keys and destroys the current decryption key before all of the decryption keys are received (e.g., for a set of N decryption keys, the customer processing platform may receive decryption keys 1 to X, where X < N, such that after receiving the second decryption key and decrypting the first encrypted section the first decryption key may be deleted at any time before the last decryption key N is received).

By having at least two decryption keys of the plurality of decryption keys, without simultaneously having possession of all of the decryption keys, as recited in independent claim 34, the customer processing platform is able to process the encrypted data content in a manner that allows for uninterrupted contiguous playback of encrypted video content, while ensuring that the customer processing platform never has a complete set of decryption keys, thereby preventing unauthorized decryption and playback of the encrypted data content. No combination of Peterka et al., Feig et al. and Giroux et al. provides the foregoing features of independent claim 34.

In view of the foregoing, Applicant respectfully submits that the rejection of independent claim 34 under 35 U.S.C. 103(a) based on Peterka et al., Feig et al. and Giroux et al. should be reconsidered and withdrawn.

Dependent Claim 56

Based at least on its dependence from independent claim 34, Applicant respectfully submits that the rejection of dependent claim 56 under 35 U.S.C. 103(a) should be reconsidered and withdrawn for at least the same reasons as the rejection of independent claim 34.

In addition, Applicant respectfully submits that Peterka et al., Feig et al.

and Giroux et al. fail to teach or even suggest "for each subsequent portion of the encrypted data: receiving a request from the customer data content processing device for the different key to decrypt the subsequent portion of the encrypted data, wherein the request was generated responsive to one of a control signal and a data pattern in the decrypted data content of a preceding portion of the encrypted data content during playback of the preceding portion of the encrypted data content.", as recited in claim 56 (emphasis added). In support of the rejection of claim 56 under 35 U.S.C. 103(a) the Examiner asserts that Feig et al. teaches the foregoing feature of claim 56. In support of this assertion the Examiner points to column 7, line 35 to column 8 line 15 of Feig et al. in paragraph 39 of the Final Action dated March 10, 2010. However, Applicant respectfully submits that the teachings of Feig et al. are completely silent with respect to the foregoing feature of claim 56.

With reference to the cited portion of Feig et al., a significant portion of which is quoted above with respect to the Examiner's similar rejection of claim 55, it should be immediately clear that it relates to the embedding of sequence numbers in the token keys (decryption keys) disclosed in Feig et al., whereas claim 56 recites "wherein the request was generated responsive to one of a control signal and a data pattern in the decrypted data content of a preceding portion of the encrypted data content during playback of the preceding portion of the encrypted data content". Applicant respectfully submits that it is entirely inappropriate to equate sequence numbers embedded in token keys, as taught by Feig et al., with a control signal or a data pattern in decrypted data content. In fact, the cited portion of Feig et al. merely states that token keys can be retrieved from the token key block (which contains all of the token keys at the customer's receiver) in a sequence ordered by the order of occurrence of playback of each corresponding encrypted section. Applicant respectfully submits that the cited portion of Feig et al. is entirely silent with respect to making a request for a next key responsive to the embedded sequence numbers, let alone responsive to one of a control signal and a data pattern in the decrypted data content, as recited in claim 56.

Furthermore, please note that the section of Feig et al. that the Examiner has pointed to in support of the rejection of claim 56 explicitly states that "only after all of the token keys are received can any viewing take place", i.e. the customer has simultaneous possession of all of the token keys, which is entirely contrary to claimed invention.

In view of the foregoing, Applicant respectfully submits that the rejection of claim 56 under 35 U.S.C. 103(a) should be reconsidered and withdrawn.

Conclusions

With respect to each of the issues presented herein for review, Applicant respectfully submits that errors have been made in the rejection of the appealed claims.

Regarding the issue of whether claims 16-23, 34 and 54-56 are unpatentable under 35 U.S.C. 112, first paragraph, Applicant respectfully requests that the rejection of claims 16-23, 34 and 54-56 be reconsidered by the Board and withdrawn.

Regarding the issue of whether claims 16-23, 34 and 54-56 are unpatentable under 35 U.S.C. 112, second paragraph, Applicant respectfully requests that the rejection of claims 16-23, 34 and 54-56 be reconsidered by the Board and withdrawn.

Regarding the issue of whether claims 16-18, 21, 54 and 55 are unpatentable under 35 U.S.C. 103(a) over Feig et al. (U.S. Patent No. 7,251,833 B2) in view of Giroux et al. (U.S. Patent Application Publication No. 2002/0078361 A1), Applicant respectfully requests that the rejection of claims 16-18, 21, 54 and 55 be reconsidered by the Board and withdrawn.

Regarding the issue of whether claim 19 is unpatentable under 35 U.S.C. 103(a) over Feig et al. in view of Giroux et al. and further in view of Granger et al. (U.S. Patent No. 6,334,189 B1), Applicant respectfully requests that the rejection of this claim be reconsidered by the Board and withdrawn.

Regarding the issue of whether claims 22 and 23 are unpatentable under 35 U.S.C. 103(a) over Feig et al. in view of Giroux et al. and further in view of Watanabe et al. (U.S. Patent No. 7,114,073 B2), Applicant respectfully requests that the rejection of claim 22 and 23 be reconsidered by the Board and withdrawn.

Regarding the issue of whether claim 20 is unpatentable under 35 U.S.C. 103(a) over Feig et al. in view of Giroux et al. and further in view of Novak (U.S. Patent Application Publication No. 2003/0097655), Applicant respectfully requests that the rejection of this claims be reconsidered by the Board and withdrawn.

Regarding the issue of whether claims 34 and 56 are unpatentable under 35 U.S.C. 103(a) over Peterka (U.S. Patent Application Publication No. 2002/0170053) in view of Feig et al. and further in view of Giroux et al., Applicant respectfully requests that the rejection of claims 34 and 56 be reconsidered by the Board and withdrawn.

Respectfully submitted,

VINCENT SO

By ____________

Allan Brett
Reg. No. 40,476
Tel.: (613) 232-2486 ext. 323

Date: June 9, 2010
RAB:JFS

Claims Appendix

1. (Withdrawn) A method of delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections;

delivering the plurality of encrypted sections to the customer processing platform; and

delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein delivering the plurality of decryption keys comprises:

delivering to the customer processing platform a current key of the plurality of decryption keys;

delivering to the customer processing platform a next key of the plurality of decryption keys; and

causing the current key to be destroyed at the customer processing platform only after at least the next key of the plurality of decryption keys has been received.

2. (Cancelled)

3. (Cancelled)

4. (Withdrawn) The method of claim 1, wherein delivering to the customer processing platform a next key of the plurality of decryption keys and causing the current key to be

destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed.

5. (Withdrawn) The method of claim 1, wherein the current encrypted section is a first one of the plurality of encrypted sections, and wherein delivering to the customer processing platform a next key of the plurality of decryption keys and causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section.

6. (Withdrawn) The method of claim 1, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

providing key control software to the customer processing platform, the key control software being adapted to:

receive the current decryption key for the current encrypted section of the plurality of encrypted sections;

receive the next decryption key for the next encrypted section of the plurality of encrypted sections;

complete decryption of the current section;

begin decryption of the next section; and

destroy the current decryption key after decryption of the next section has begun.

7. (Withdrawn) The method of claim 1 further comprising:

billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform.

8. (Withdrawn) The method of claim 1, wherein the data content is video content or music content, and wherein use of the data content at the customer processing platform comprises decryption and playback of the data content.

9. (Withdrawn) The method of claim 1, wherein each of the plurality of encryption keys comprises a respective symmetric cryptographic key, and wherein each of the plurality of decryption keys comprises the symmetric cryptographic key of its corresponding encryption key.

10. (Withdrawn) The method of claim 1, further comprising:

generating each of the plurality of encryption keys using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing platform-specific keys.

11. (Withdrawn) The method of claim 10, wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value.

12. (Withdrawn) The method of claim 11, wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values.

13. (Withdrawn) The method of claim 1, further comprising:

generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with the customer processing platform,

wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the transmission values.

14. (Withdrawn) The method of claim 1, further comprising:

delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform via a peer-to-peer network; and

delivering the plurality of decryption keys from the data content provider to the second customer processing platform, wherein the decryption keys are delivered in a manner such that the second customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein the plurality of decryption keys are encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform.

15. (Withdrawn) A computer-readable medium storing instructions which, when executed by a processor at a data content provider, perform a method according to claim 1.

16. (Previously Presented) A method of receiving and controlling playback of video data content at a customer processing platform, comprising:

receiving over a communications medium a plurality of encrypted sections of video data content, each of which has been encrypted using a respective encryption key; and

for each encrypted section:

receiving a respective decryption key in respect of the encrypted section before playback of a preceding encrypted section of the plurality of encrypted sections is complete;

decrypting and playing back the encrypted section using the respective decryption key; and

destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content.

17. (Previously Presented) The method of claim 16, further comprising, for each encrypted section:

destroying decrypted video data content at the customer processing platform after completing playback of the encrypted section.

18. (Original) The method of claim 16, wherein the communications medium is the public Internet.

19. (Previously Presented) The method of claim 16, wherein, for each encrypted section, the respective encryption key is the same as the respective decryption key.

20. (Previously Presented) The method of claim 16, wherein receiving the plurality of encrypted sections of the video data content comprises receiving the plurality of encrypted sections of the video data content from another customer processing platform via a peer-to-peer network, and wherein, for each encrypted section, the decryption key is encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform.

21. (Original) A computer-readable medium storing instructions which, when executed by a customer processing platform, perform a method according to claim 16.

22. (Original) The method of claim 16, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform.

23. (Previously Presented) The method of claim 16, wherein receiving each respective decryption key comprises receiving a transmission value that is determined based on the respective decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section:

recovering the respective decryption key from the transmission value.

24.–33.(Cancelled)

34. (Previously Presented) A method for controlling use of encrypted video data content downloaded to a customer data content processing device, comprising:

receiving a request comprising customer verification information from a customer data content processing device;

comparing the customer verification information with corresponding stored customer information; and where the customer verification information is consistent with the stored customer verification information:

billing a usage charge to an account of the customer;

transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted video data content; and

for each subsequent portion of the encrypted video data content:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted video data content before playback of a preceding portion of the encrypted video data content is complete; and

causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device only after at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device, such that contiguous playback of the portions of encrypted video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted video data content.

35. (Withdrawn) A computer readable medium storing software code executable by a processing platform, the software code comprising:

first software code for coordinating downloading a plurality of sections of data content each encrypted with a respective one of a plurality of encryption keys to a customer computer system from a data content service provider system or another customer computer system; and

second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decryption keys such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein for each encrypted section of data content the second software code destroys the received decryption key corresponding to the encrypted section of data content only after receiving at least the decryption key corresponding to the next encrypted section of data content.

36. (Withdrawn) The computer readable medium of claim 35, wherein the second software code obtains further permissions from the data content service provider system to continue using the data content.

37. (Cancelled)

38. (Withdrawn) A system for delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

means for encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections;

means for delivering the plurality of encrypted sections to the customer processing platform; and

means for delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein the means for delivering the plurality of decryption keys comprises:

means for delivering to the customer processing platform a current key of the plurality of decryption keys; and

means for delivering to the customer processing platform a next key of the plurality of decryption keys, the customer processing platform comprising:

means for destroying the current key at the customer processing platform only after at least the next key of the plurality of decryption keys has been received.

39. (Withdrawn) The system of claim 38, wherein the customer processing platform comprises:

means for requesting the data content to be delivered to the customer processing platform via a peer-to-peer network connection;

means for receiving the plurality of encrypted sections via the peer-to-peer network connection;

means for receiving, for each encrypted section, the decryption key in respect of the encrypted section over an encrypted decryption key delivery channel; and

means for decrypting and playing back the encrypted section using the decryption key, wherein

the means for destroying the current decryption key comprises means for destroying the current decryption key~~,~~ after completing playback of the current encrypted section and beginning playback of the next encrypted section.

40. (Withdrawn) A data content distribution system comprising:

a data content server configured to receive download requests and permission requests for data content, to encrypt a plurality of sections of requested data content using respective encryption keys to thereby generate a plurality of encrypted sections and to transmit the encrypted sections of the data content in response to a received download request for the data content, and to transmit each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content; and

a data content download controller configured to generate download requests, to receive encrypted sections of data content in response to download requests, to generate permission requests when downloaded data content is to be used, and for each encrypted section of data content to be used, to receive a corresponding one of the plurality of decryption keys, and to decrypt the encrypted section using the corresponding one of the plurality of decryption keys; said data content server operable to transmit the plurality of decryption keys in a manner such that the data content download controller has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein, for each encrypted section, the data content download controller destroys the decryption key corresponding to the encrypted section only after at least the decryption key corresponding to the next encrypted section of the plurality of encrypted sections has been received.

41. (Withdrawn) The system of claim 40, comprising a data network connecting the data content server and the data content download controller.

42. (Withdrawn) The system of claim 41, further comprising a plurality of data content download controllers connected to the data network.

43. (Withdrawn) The system of claim 42, wherein each of the plurality of data content download controllers is implemented in conjunction with a respective customer computer system and is further configured to download encrypted sections of data content from other customer computer systems.

44. (Withdrawn) The method of claim 1, wherein causing the current key to be destroyed at the customer processing platform comprises:

causing the current key to be destroyed at the customer processing platform after processing of the current encrypted section of the plurality of encrypted sections with the current key has been completed and processing of a next encrypted section of the plurality of encrypted sections with the next key has begun.

45. (Withdrawn) The method of claim 1, wherein causing the current key to be destroyed at the customer processing platform comprises:

causing the current key to be destroyed at the customer processing platform before processing of the next encrypted section has been completed.

46. (Withdrawn) The method of claim 1, wherein:

delivering to the customer processing platform a plurality of decryption keys comprises:

delivering the plurality of decryption keys to the customer processing platform over an encrypted decryption key delivery channel; and

delivering the plurality of encrypted sections to the customer processing platform comprises:

providing the plurality of encrypted sections to a peer-to-peer network, wherein the customer processing platform downloads the plurality of encrypted sections via the peer-to-peer network.

47. (Withdrawn) The method of claim 34, wherein causing a key for a preceding portion of the encrypted data to be deleted comprises:

causing the key for the preceding portion of the encrypted data to be deleted from the customer data content processing device only after decryption of the subsequent portion of the encrypted data has begun.

48. (Withdrawn) The computer readable medium of claim 35, wherein the second software code destroys the received decryption key corresponding to the encrypted section of data content only after decryption of the next encrypted section of data content has begun.

49. (Withdrawn) The system of claim 38, wherein the means for causing the current key to be destroyed at the customer processing platform comprises:

means for causing the current key to be destroyed at the customer processing platform after processing of the current encrypted section of the plurality of encrypted sections with the current key has been completed and processing of a next encrypted section of the plurality of encrypted sections with the next key has begun.

50. (Withdrawn) The system of claim 38, wherein the means for causing the current key to be destroyed at the customer processing platform comprises:

means for causing the current key to be destroyed at the customer processing platform before processing of the next encrypted section has been completed.

51. (Withdrawn) The system of claim 38, wherein:

the means for delivering to the customer processing platform a plurality of decryption keys comprises:

means for delivering the plurality of decryption keys to the customer processing platform over an encrypted decryption key delivery channel; and

the means for delivering the plurality of encrypted sections to the customer processing platform comprises:

a peer-to-peer network, wherein the customer processing platform downloads the plurality of encrypted sections via the peer-to-peer network.

52. (Withdrawn) The system of claim 40, wherein the data content download controller destroys the decryption key corresponding to the encrypted section only after decryption of the encrypted section has completed and decryption of the next encrypted section of the plurality of encrypted sections with the decryption key corresponding to the next encrypted section of the plurality of encrypted sections has begun.

53. (Withdrawn) The system of claim 43, comprising an encrypted decryption key channel for delivery of the plurality of decryption keys, wherein the data network comprises a peer-to-peer network connecting the customer computer systems to share the encrypted sections of data content, and wherein the encrypted decryption key channel is separate from the peer-to-peer network.

54. (Previously Presented) The method of claim 16, wherein destroying the respective decryption key only after at least the respective decryption key in respect of the next encrypted section has been received comprises destroying the respective decryption key only after completing playback of the encrypted section and beginning contiguous playback of the next encrypted section.

55. (Previously Presented) The method of claim 16, further comprising, for each encrypted section:

requesting the respective decryption key in respect of a next encrypted section responsive to one of a control signal and a data pattern in the decrypted data content of an encrypted section that precedes the next encrypted section.

56. (Previously Presented) The method of claim 34, further comprising, for each subsequent portion of the encrypted data:

receiving a request from the customer data content processing device for the different key to decrypt the subsequent portion of the encrypted data, wherein the request was generated responsive to one of a control signal and a data pattern in the decrypted data content of a preceding portion of the encrypted data content during playback of the preceding portion of the encrypted data content.

Evidence Appendix

None

Related Proceedings Appendix

None